



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO.             | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------------------|-------------|----------------------|---------------------|------------------|
| 10/628,006                  | 07/25/2003  | Brian Hornacki       | SYMAP027            | 3957             |
| 21912                       | 7590        | 06/26/2007           | EXAMINER            |                  |
| VAN PELT, YI & JAMES LLP    |             |                      | CALLAHAN, PAUL E    |                  |
| 10050 N. FOOTHILL BLVD #200 |             |                      | ART UNIT            | PAPER NUMBER     |
| CUPERTINO, CA 95014         |             |                      | 2137                |                  |
|                             |             |                      | MAIL DATE           | DELIVERY MODE    |
|                             |             |                      | 06/26/2007          | PAPER            |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

|                              |                 |                 |
|------------------------------|-----------------|-----------------|
| <b>Office Action Summary</b> | Application No. | Applicant(s)    |
|                              | 10/628,006      | HERNACKI, BRIAN |
|                              | Examiner        | Art Unit        |
|                              | Paul Callahan   | 2137            |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

1) Responsive to communication(s) filed on 02 April 2007.  
 2a) This action is **FINAL**.                            2b) This action is non-final.  
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

4) Claim(s) 1-7,9-18,20 and 21 is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) Claim(s) \_\_\_\_\_ is/are allowed.  
 6) Claim(s) 1-7,9-18,20 and 21 is/are rejected.  
 7) Claim(s) \_\_\_\_\_ is/are objected to.  
 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

9) The specification is objected to by the Examiner.  
 10) The drawing(s) filed on 02 April 2007 is/are: a) accepted or b) objected to by the Examiner.  
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) All    b) Some \* c) None of:  
 1. Certified copies of the priority documents have been received.  
 2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

1) Notice of References Cited (PTO-892)  
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)  
 3) Information Disclosure Statement(s) (PTO/SB/08)  
 Paper No(s)/Mail Date \_\_\_\_\_

4) Interview Summary (PTO-413)  
 Paper No(s)/Mail Date. \_\_\_\_\_ .  
 5) Notice of Informal Patent Application  
 6) Other: \_\_\_\_\_.

### **DETAILED ACTION**

1. Claims 1-22 were pending in the instant application at the time of the previous Office Action, mailed January 11, 2007. By the latest amendment, filed April 2, 2007, claims 8, 19, and 22 have been cancelled. Therefore claims 1-7, 9-18, 20, and 21 remain pending and have been examined.

#### ***Response to Arguments***

2. Applicant's arguments with respect to claims 1-7, 9-18, 20, and 21 have been considered but are moot in view of the new ground(s) of rejection.

#### ***Drawings***

3. The drawings were received on April 2, 2007. These drawings are approved.

#### ***Claim Rejections - 35 USC § 103***

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1-7, 9-18, 20 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gupta et al., US 2003/0004688 A1, and Stellenberg et al., US 7,134,143.

As for Claim 1, Gupta teaches a method for identifying network traffic [0002] comprising: receiving pattern matching data [0043]; comparing the pattern matching data with a pattern [0050], [0084]; and determining whether the pattern matching data matches the pattern [0087]. Gupta does not teach the features of assigning a first score to a first match if the pattern matching data matches the pattern, and comparing the pattern matching data with a second pattern; and assigning a second score to a second match if the pattern matching data matches a second pattern. However, Stellenberg does teach these features (col. 4 lines 7-18, 30-35, col. 19 lines 20-47). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate these features into the system of Gupta. It would have been desirable to do so as this would provide for a second level of filtering of potentially harmful network traffic.

As for claim 2, Gupta teaches a method for identifying network traffic as recited in Claim 1, wherein the pattern matching data includes application data [0076], [0081], [0083], [0095].

As for claim 3, Gupta teaches a method for identifying network traffic as recited in Claim 1, in the event that the pattern matching data matches the pattern, further including determining a property associated with the network traffic [0063], [0064].

As for claim 4, Gupta teaches a method for identifying network traffic as recited in Claim 1, in the event that the pattern matching data matches the pattern, further including determining a property associated with the network traffic; wherein the property is an application protocol [0063], [0064].

As for claim 5, Gupta teaches a method for identifying network traffic as recited in Claim 1, in the event that the data matches the pattern, further including determining a property associated with the data and assigning a score for the property [0055], [0059].

As for claim 6, Gupta teaches a method for identifying network traffic as recited in Claim 1, in the event that the data matches the pattern, further including determining a property associated with the data; and applying a policy based on the property [0055], [0059], [0061].

As for claim 7, Gupta teaches a method for identifying network traffic as recited in Claim 1, further comprising assigning a score to a match if the pattern matching data matches the pattern [0055].

As for claim 9, Gupta fails to teach the method for identifying network traffic as recited in claim 1 further comprising determining a property associated with the traffic by comparing the first score and the second score (col. 19 lines 20-47).

As for claim 10, Gupta teaches a method for identifying network traffic as recited in Claim 1, wherein the pattern matching data includes a string selected from a packet [0084], [0085], [0086].

As for claim 11, Gupta teaches a method for identifying network traffic as recited in Claim 1, wherein pattern matching data includes concatenated application data of a plurality of packets [0068], [0104].

As for claim 12, Gupta teaches a method for identifying network traffic as recited in Claim 1, wherein the pattern includes a regular expression [0076], [0081], [0083], [0095].

As for claim 13, Gupta teaches a method for identifying network traffic as recited in Claim 1, wherein the pattern includes application protocol information [0063], [0064].

As for claim 14, Gupta teaches a method for identifying network traffic as recited in Claim 1, wherein the pattern includes commonly used port information [0076], [0107].

As for claim 15, Gupta teaches a method for identifying network traffic as recited in Claim 1, in the event the data does not match the pattern, further comprising returning a failure indicator [0104: Alert].

As for claim 16, Gupta teaches a method for identifying network traffic as recited in Claim 1, wherein determining whether the pattern matching data matches the pattern occurs at the beginning of session [0103: Packet is cached and analyzed upon receipt].

As for claim 17, Gupta teaches a method for identifying network traffic as recited in Claim 1, wherein comparing the pattern matching data with a pattern is performed for each received data [0103].

As for Claim 18, Gupta teaches a method for identifying network traffic [0002] comprising: receiving pattern matching data [0043]; comparing the pattern matching data with a pattern [0050], [0084]; and determining whether the pattern matching data matches the pattern [0087]. Gupta does not teach comparing the pattern matching data with a second pattern; and assigning a second score to a second match if the pattern matching data matches a second pattern. However, Stellenberg does teach these features (col. 4 lines 7-18, 30-35, col. 19 lines 20-47). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate these features into the system of Gupta. It would have been desirable to do so as this would provide for a second level of filtering of potentially harmful network traffic.

Claim 20 is directed towards a system that carries out the method steps of claim 1.

Claim 20 recites substantially the same limitations as claim 1 and therefore is rejected on the same basis as that claim.

Claim 21 is directed towards a computer program embodied in a computer-readable medium that causes a processor to undertake the method steps of claim 1.

Claim 21 recites substantially the same limitations as claim 1 and therefore is rejected on the same basis as that claim.

### ***Conclusion***

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (571) 272-3869. The examiner can normally be reached on M-F from 9 to 5.

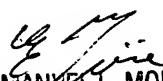
If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, Emmanuel Moise, can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is: (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should

you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Paul Callahan

/Paul E. Callahan/  
6-21-07

  
EMMANUEL L. MOISE  
SUPERVISORY PATENT EXAMINER